

SonicWALL Content Security Manager Series

**SonicWALL CSM 2200**

**Getting Started Guide**



# SonicWALL Content Security Manager 2200 Getting Started Guide

Thank you for purchasing a SonicWALL Content Security Manager (CSM) series appliance. The SonicWALL CSM is an Internet content and application filter that enhances security and employee productivity, optimizes network bandwidth and mitigates legal liabilities. The SonicWALL CSM integrates into virtually any network to provide powerful, scalable, cost-effective Internet content filtering that is easy to implement, requiring no change to your network clients. The SonicWALL CSM filters HTTP traffic on any port, regardless of whether the network clients use external proxy servers.



---

**Note:** For complete instructions, refer to the SonicOS CF 2.5 Administrator's Guide. For solutions using SonicWALL ADConnector, refer to the SonicWALL Content Security Manager Integrated Solutions Guide, available on the SonicWALL CSM Resource CD and at <http://www.sonicwall.com/support/documentation.html>.

---

## Contents

This getting started guide contains the following sections:

- “Before You Begin” on page 2
  - “Check Package Contents” on page 3
  - “What You Need to Provide” on page 4
  - “Important Information You Need” on page 4
  - “SonicWALL CSM 2200 Front and Back Panels Overview” on page 5
- “Configuring Your SonicWALL CSM” on page 6
  - ① “Applying Power to the SonicWALL CSM” on page 6
  - ② “Accessing the SonicWALL Management Interface” on page 7
  - ③ “Configuring Your SonicWALL CSM Using the Setup Wizard” on page 9
  - ④ “Connecting the SonicWALL CSM to Your Network” on page 14
  - ⑤ “Registering Your SonicWALL CSM” on page 17
  - ⑥ “Understanding the \*Default Policy” on page 21
  - ⑦ “Verifying the \*Default Policy” on page 23
  - ⑧ “Integrating the SonicWALL CSM with Microsoft Active Directory” on page 24
- “Advanced Configuration” on page 32

## Before You Begin

This section contains the following subsections:

- “Check Package Contents” on page 3
- “What You Need to Provide” on page 4
- “Important Information You Need” on page 4
- “SonicWALL CSM 2200 Front and Back Panels Overview” on page 5

## Check Package Contents

1. One SonicWALL SonicWALL CSM appliance
2. One SonicWALL CSM Getting Started Guide
3. One SonicOS Release Note
4. One Thank You card
5. One straight-through Ethernet cable
6. One red crossover Ethernet cable
7. One power cord\*
8. One SonicWALL CSM Resource CD
9. Rack mounting hardware

*\*The power cord is for North America use only.*

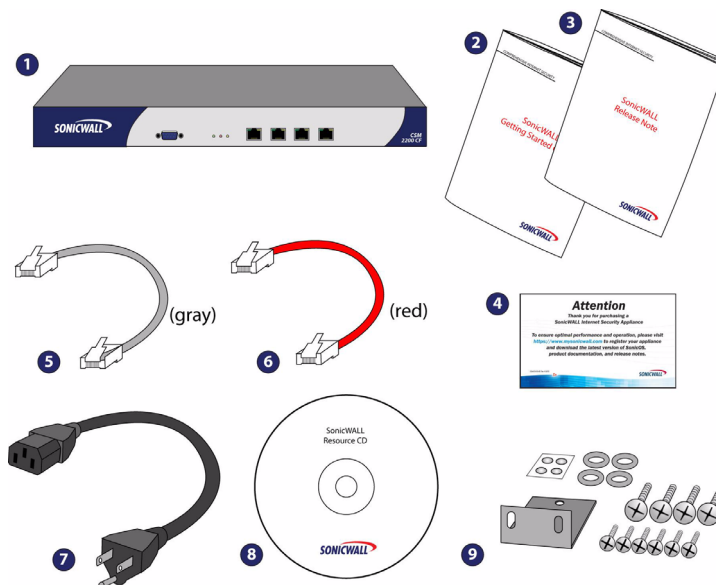
*\* Das eingeschlossene Netzkabel ist für Gebrauch in Nordamerikas nur vorgehabt. Für Europäische Union (EU) Kunden, ist ein Netzkabel nicht eingeschlossen.*



---

**Note:** SonicWALL ADConnector and SonicWALL ViewPoint software for the SonicWALL CSM are available for download from the SonicWALL Web site <https://www.mysonicwall.com>.

---



## What You Need to Provide

- A firewall or security appliance protecting your LAN
- PC or Macintosh computer to act as an out-of-band management station for initial configuration of the SonicWALL CSM
- Web browser for accessing the SonicWALL CSM's Web-based management interface. The Web browser must support Java and HTTP uploads. Internet Explorer 5.0 or higher or Netscape Navigator 4.7 or higher are recommended.

## Important Information You Need

### LAN

LAN IP address range: \_\_\_\_\_

LAN netmask: \_\_\_\_\_

DNS server: \_\_\_\_\_

### Firewall or Security Appliance

Firewall or router gateway IP address: \_\_\_\_\_

Firewall or security appliance management IP address: \_\_\_\_\_

### mySonicWALL.com Account

This is sensitive information. Store this information carefully.

Username: \_\_\_\_\_

Password: \_\_\_\_\_

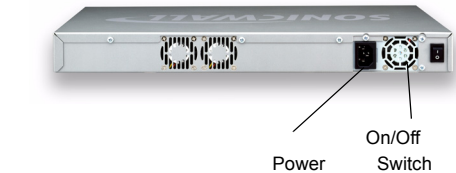
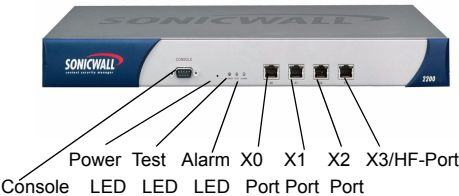
### SonicWALL CSM Management Account

This is sensitive information. Store this information carefully.

Username: \_\_\_\_\_ (default: *admin*)

Password: \_\_\_\_\_ (default: *password*)

# SonicWALL CSM 2200 Front and Back Panels Overview



Front Panel Feature	Description
<b>Console</b>	Provides access to command-line interface.
<b>Power LED</b>	Indicates the SonicWALL CSM appliance is powered on.
<b>Test LED</b>	Indicates the SonicWALL CSM appliance is in test mode.
<b>Alarm LED</b>	Indicates a critical error or failure.
<b>X0 Port</b>	Provides a connection to your LAN.
<b>X1 Port</b>	Provides a primary (Ethernet) connection to the Internet.
<b>X2 Port</b>	Provides a connection for out-of-band management. This port has no network connection.
<b>X3/HF-Port</b>	Provides an optionally configurable HF (hardware failover) port. Note: This port is not configurable for other types of connections.

Back Panel Feature	Description
<b>Power</b>	Provides power connection using supplied power cord.
<b>On/Off Switch</b>	Powers the SonicWALL CSM appliance on and off.

# Configuring Your SonicWALL CSM

Configuring your SonicWALL CSM comprises the following steps:

- 1 “Applying Power to the SonicWALL CSM” on page 6
- 2 “Accessing the SonicWALL Management Interface” on page 7
- 3 “Configuring Your SonicWALL CSM Using the Setup Wizard” on page 9
- 4 “Connecting the SonicWALL CSM to Your Network” on page 14
- 5 “Registering Your SonicWALL CSM” on page 17
- 6 “Understanding the \*Default Policy” on page 21
- 7 “Verifying the \*Default Policy” on page 23
- 8 “Integrating the SonicWALL CSM with Microsoft Active Directory” on page 24



---

**Note:** After step 7, the SonicWALL CSM is fully functional, using the built-in \*Default Policy to filter content. Continue to step 8 to further customize your installation.

---

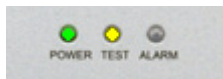
## 1

### Applying Power to the SonicWALL CSM

To apply power to your SonicWALL CSM appliance:

1. Plug the power cord into the back panel of the SonicWALL CSM and into an appropriate power outlet.
2. Turn on the SonicWALL CSM appliance using the On/Off switch located on the back panel of the appliance.

The Power LED shines green when you activate the power switch. The Test LED and Alarm LED light up and may blink while the appliance performs a series of diagnostic tests. When the Test LED and Alarm LED are no longer lit, the SonicWALL CSM is ready for configuration.



## 2

## Accessing the SonicWALL Management Interface

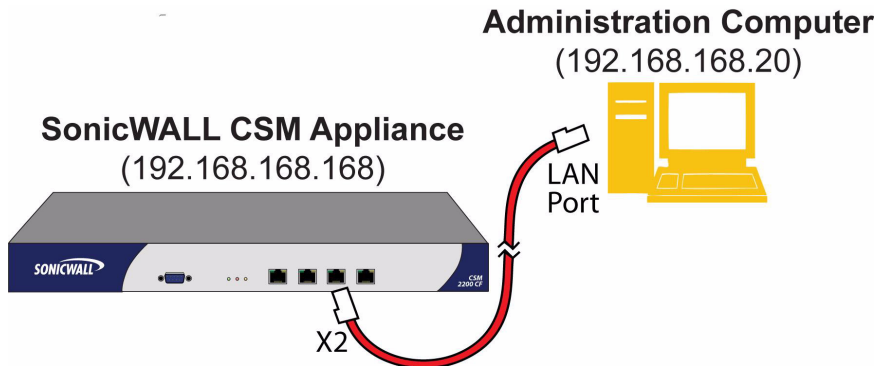
To access the Web-based management interface of the SonicWALL CSM, configure your out-of-band management station (the computer you are using to manage the SonicWALL CSM) with the following static TCP/IP address properties:

- IP address: **Use an available IP address on the 192.168.168.0/24 subnet. For example, 192.168.168.20.**
- Subnet mask: **255.255.255.0**
- DNS settings: **You do not need to configure the default gateway or DNS settings.**

For help configuring a static IP address, refer to “Configuring Static IP” on page 33.

When you have configured the static IP address and subnet mask on your management station, perform the following steps to access the SonicWALL CSM management interface:

1. Connect one end of the red crossover Ethernet cable to the Ethernet port of the out-of-band management station. Connect the other end of the red crossover cable to the **X2** port on the SonicWALL CSM.



---

**Note:** The **X2** port is for out-of-band management and has no network connection.

---

2. Start your Web browser.



---

**Alert:** Your Web browser must support Java and HTTP uploads. Internet Explorer 5.0 or higher or Netscape Navigator 4.0 or higher are recommended.

---



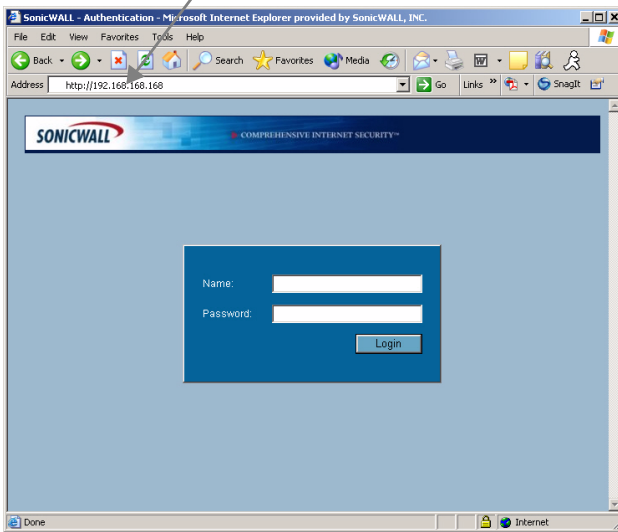
3. Enter **http://192.168.168.168** in the **Location** or **Address** field and press **Enter** on your keyboard.



---

**Note:** *For additional security, you may also access the appliance using HTTPS.*

---



4. In the SonicWALL CSM authentication page, enter *admin* in the **Name** field and *password* in the **Password** field and click **Login**. The **Setup Wizard** page is displayed.
5. Unable to connect?  
If you cannot connect to the SonicWALL CSM, verify the following configurations:
  - Did you correctly enter the SonicWALL CSM X2 management IP address, **http://192.168.168.168**, in your Web browser?
  - Did you change the TCP/IP network settings on your computer?
  - Did you use the red crossover Ethernet cable to connect your out-of-band management station to the **X2** (out-of-band management) port on your SonicWALL CSM?

## 3

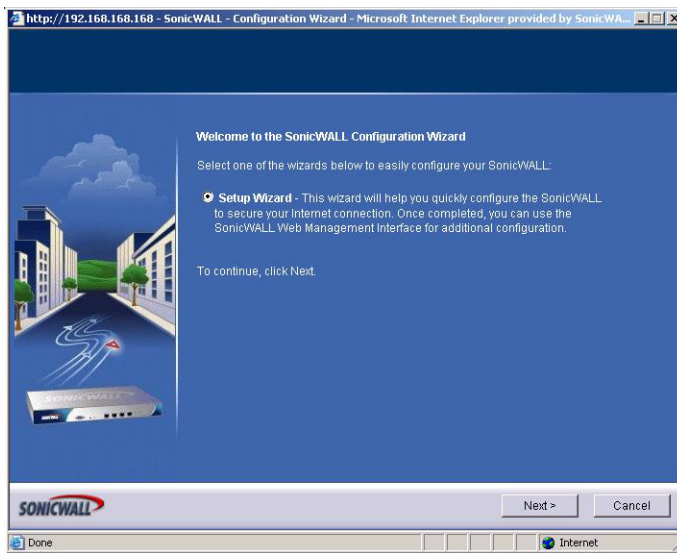
## Configuring Your SonicWALL CSM Using the Setup Wizard

The SonicWALL CSM Setup Wizard page automatically displays after the CSM is properly powered on and configured for and connected to your management station. The Setup Wizard allows you to configure the following components:

- Password
- Time zone
- Network setup

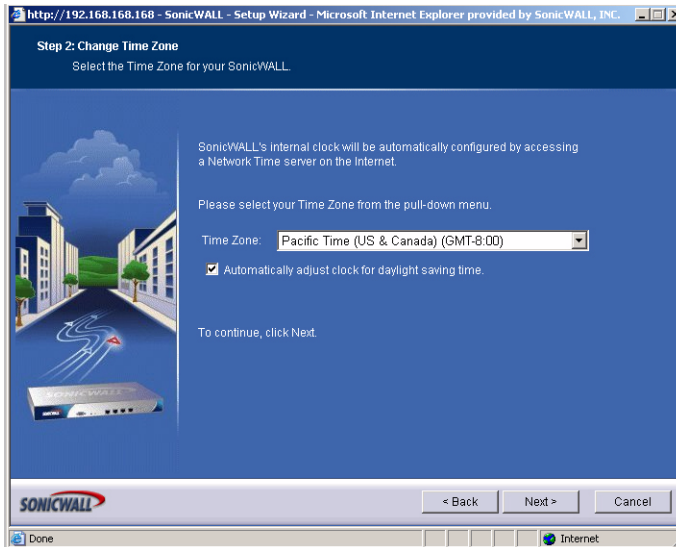
To configure your SonicWALL CSM using the Setup Wizard, perform the following steps:

1. The SonicWALL Setup Wizard will automatically launch.
2. The **Welcome to the SonicWALL Configuration Wizard** screen displays. Confirm that the radio button next to Setup Wizard is selected and click **Next>** to continue.



3. In the **Change Password** screen, you will be prompted to create a new password. The **Old Password** is pre-populated. Enter a new password in the **New Password** field and re-enter it in the **Confirm** field. Click **Next>** to continue. Passwords are case-sensitive.

4. In the **Time Zone** drop down list, select the correct time zone for your location. Check the box next to **Automatically adjust clock for daylight saving time** if you live in a region that observes Daylight Saving Time. Click **Next>** to continue.



---

**Note:** *For best performance, you need to configure the time zone to accurately reflect geographic location. It is important that you set the time zone correctly before you register your SonicWALL CSM appliance.*

---

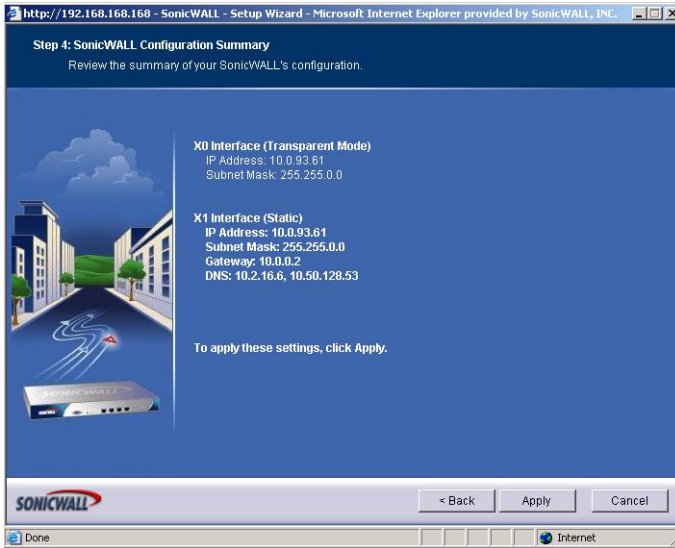
5. The **Network Setup** screen will prompt you for information to configure the SonicWALL CSM's **X0** and **X1** interfaces, which will enable Internet connectivity. Refer to the table below for a description of the Network Setup fields. After you have entered the required information, press **Next>** to continue.



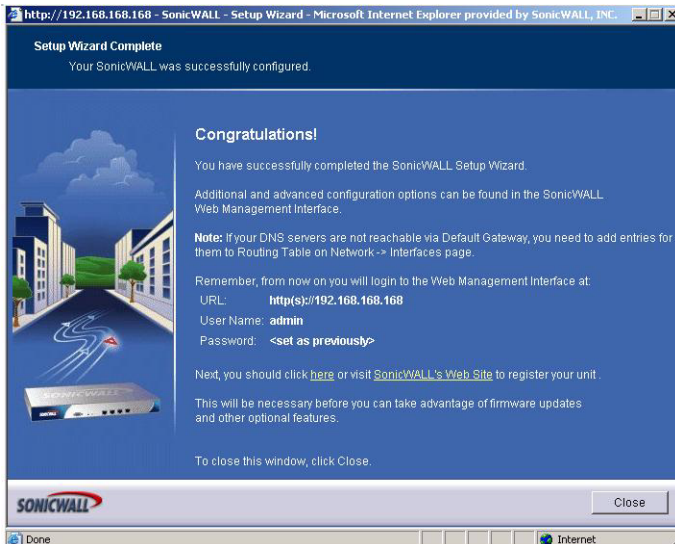
**Alert:** You must configure the network interfaces before connecting the SonicWALL CSM to your network. If you have already connected cables to the **X0** and **X1** interfaces, disconnect them before continuing this step.

Field	Description
SonicWALL WAN <u>IP Address</u>	Enter a single, static IP address to assign to the SonicWALL CSM appliance. Make sure this address will not be assigned to any other device.
WAN <u>Subnet Mask</u>	Enter the subnet mask for your network. For example, 255.255.0.0.
<u>Gateway</u> (Router) Address	Enter the default gateway of your network.
DNS Server Address	Enter the DNS server address for your network.
DNS Server Address #2 (optional)	Enter a secondary, back-up DNS server to use if the first one fails.

6. The **SonicWALL Configuration Summary** displays. Click **Apply** to confirm the settings. After you click the Apply button, the **Storing SonicWALL Configuration** screen displays. It may take up to two minutes while changes are being applied to your SonicWALL CSM appliance.



7. When the configuration has been stored, you will see the **Setup Wizard Complete** screen. Click **Close** to close the Wizard. Continue to "Connecting the SonicWALL CSM to Your Network" on page 14. Keep a hardcopy record of your *IP address*, *user name* and *password* for your SonicWALL CSM appliance for administrator login.



8. Disconnect your crossover cable from your management station and the CSM appliance and refer to “Connecting the SonicWALL CSM to Your Network” on page 14.



---

**Note:** *After initial configuration using the X2 out-of-band management interface, you can now perform management from the LAN (X0) interface.*

---

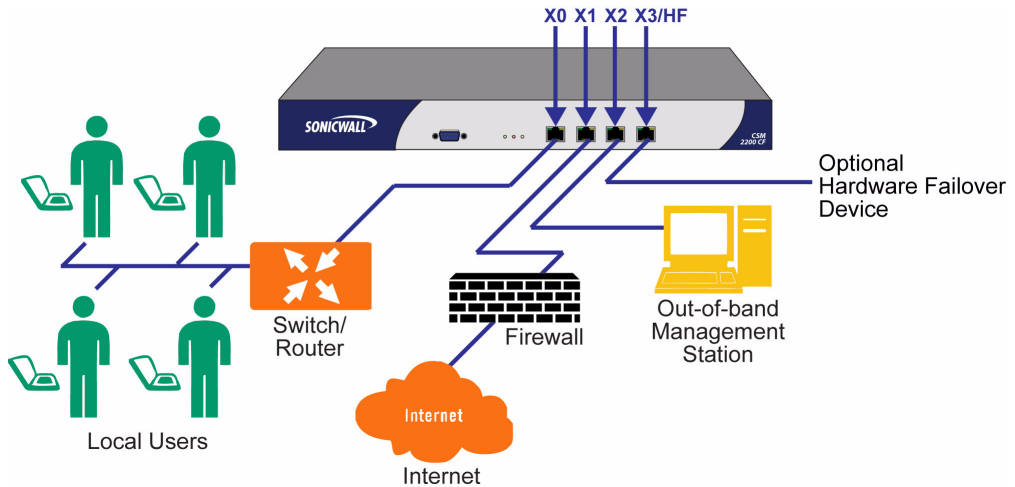
## 4

## Connecting the SonicWALL CSM to Your Network

Connect the SonicWALL CSM between your LAN and your firewall/security appliance, allowing it to filter content requests from the LAN before they pass through the firewall/security appliance. This step contains the following procedures:

- “Connecting the Ethernet Cables” on page 15
- “Testing Your Connectivity” on page 15
- “Adding Static Routes” on page 16

Figure 1: SonicWALL CSM Configuration Between the LAN and WAN



**Alert:** Do not connect the SonicWALL CSM to your network until you have configured the **X0** and **X1** interfaces. Refer to “Configuring Your SonicWALL CSM Using the Setup Wizard” on page 9.



**Note:** Before you connect the SonicWALL CSM to your network, reconfigure the TCP/IP address properties of your out-of-band management station to the original IP address and subnet mask settings.

## Connecting the Ethernet Cables

1. Connect one end of the Ethernet cable connected to your internal network (your LAN hub, switch, or router) to the **X0** (Internal) port of the SonicWALL CSM. The LEDs on the **X0** port light up indicating an active connection.
2. Connect one end of an Ethernet cable connected to your firewall or Internet connection to the **X1** (External) port of the SonicWALL CSM.

The LEDs on the **X1** port light up indicating an active connection.

## Testing Your Connectivity

1. Open a Web browser and log into the CSM management interface by typing the IP address you assigned to the SonicWALL CSM appliance in the **Address** or **Location** bar.
2. In the left-navigation menu, click **System** and then click **Diagnostics**.
3. Under Network Settings, click **Run Test**.
4. The test may take up to two minutes before the results display.

The screenshot shows the SonicWALL CSM management interface. The left sidebar contains a navigation menu with categories: System, Network, and Users and Hosts. The 'System' category is expanded, showing sub-items: Status, Licenses, Administration, Time, Schedules, Settings, Diagnostics, and Restart. The 'Diagnostics' sub-item is selected. The main content area is titled 'System > Diagnostics' and includes a 'Diagnostic Tools' section with a dropdown menu set to 'Check Network Settings' and a 'Run Test' button. Below this is a 'Check Network Settings' section with a 'Run Test' button. The 'General Network Connections' section displays a table of network settings and test results. The 'Security Management' section displays a table of security management settings and test results. The status bar at the bottom indicates 'Status: Ready' and 'Done'.

Server	IP Address	Test Results	Notes
Default Gateway	10.0.0.2	ping time 50 msec	
DNS Server 1	10.50.128.52	ping time < 10 msec	
DNS Server 2	10.50.128.53	ping time < 10 msec	
DNS Server 3	0.0.0.0	not configured	
diagnostics.sonicwall.com	67.115.118.8	ping time 50 msec	

Server	IP Address	Test Results	Notes
License Manager	64.41.135.42	ready	
Content Filtering Server	0.0.0.0	not configured	





**Tip:** The **System > Diagnostics > Run Test** page provides the status of your network connection and security services. The example on this page shows test results for a SonicWALL CSM appliance with multiple active network DNS server connections. The **Content Filtering Server** status is displayed as “not configured” in red, which accurately reflects this SonicWALL CSM appliance not having an active Content Filtering Server subscription service. Adding subscription services is discussed later in this document.

## Adding Static Routes

If you cannot connect to the firewall or router gateway or to URLs outside your firewall, and your network consists of multiple subnets, you may need to add static routes to your company routers, internal DNS servers, and your SonicWALL ADConnector. Refer to “Figure 1: SonicWALL CSM Configuration Between the LAN and WAN” on page 14.

To add static routes in the SonicWALL CSM management interface, perform the following steps:

1. In the SonicWALL CSM management interface, in the left-navigation menu, click **Network** and then click **Interfaces**.
2. In the **Network > Interfaces** page, click **Add** below the **Routing Table**.
3. The **Add Route** window is displayed.

The screenshot shows a dialog box titled "Add Route - Microsoft Internet Explorer provide...". It has four input fields: "IP Address From:", "IP Address To:", "Gateway IP:", and "Interface:". The "Interface:" dropdown menu is currently set to "Internal (X0)". At the bottom of the dialog are "OK" and "Cancel" buttons.

4. Enter the beginning IP address of the IP address range to which the DNS server or Internet gateway belongs in the **IP Address From** field.
5. Enter the ending IP address of the IP address in the **IP Address To** field.
6. Enter the IP address of the gateway device to which the DNS server or Internet gateway are attached in the **Gateway IP** field.
7. Select **Internal (X0)** or **External (X1)** from the **Interface** menu.
8. Click **OK**. The static route entry is added to the **Routing Table**.
9. The **Routing Table** displays the list of destinations that the IP software maintains on each host and router.

Routing Table			
IP Address Range	Gateway	Interface	Configure
10.0.93.10 - 10.0.93.15	10.0.93.49	X0	 
<div>Add... Delete All</div>			

## Registering Your SonicWALL CSM

Once you have established an Internet connection for your SonicWALL CSM, you must register the SonicWALL CSM to activate:

- Allowed Nodes/Users license
- SonicWALL Content Filtering Service subscription
- Client Anti-Virus
- Gateway Anti-Virus
- Anti-Spyware
- Application Filter Service subscription
- Multimedia Application Filters
- Intrusion Prevention Service
- ViewPoint

Registering your SonicWALL CSM also allows you to:

- Download related software:
  - SonicWALL ADConnector
  - SonicWALL ViewPoint
- Receive firmware updates
- Access to SonicWALL technical support
- Get subscription renewals
- Upgrade node/user licenses

## Before You Register

You need a mySonicWALL.com account to register your SonicWALL CSM. You can create a new mySonicWALL.com account directly from the SonicWALL management interface.



**Alert:** Verify that the DNS and Time settings on your SonicWALL CSM are correct when you register the device. Your DNS and Time settings should have been configured with the Setup Wizard. You can verify the Time settings in the **System > Time** page. You can verify the DNS settings from the **Network > Interfaces** page under Interface Settings by clicking the **Configure** icon next to the X1 (External) port.

**SonicWALL** Comprehensive Internet Security™

System  
Network

Interfaces  
ARP  
Web Proxy

Users and Hosts  
Policies  
Web Filters  
Application Filters  
Threat Protection  
Hardware Failover  
Log  
Wizards  
Help  
Logout

Status: Ready

### Network > Interfaces

[Clear Statistics](#) [?](#)

#### Interface Traffic Statistics

Traffic Statistic	X0	X1	X2	X3
Rx Unicast Packets:	200437	2555848	0	0
Rx Broadcast Packets:	5004	4975988	0	0
Rx Bytes:	38000514	2871057762	0	0
Tx Unicast Packets:	253945	265749	0	0
Tx Broadcast Packets:	4961569	8691	0	0
Tx Bytes:	1758780175	42092573	0	0

#### Interface Settings

Name	Zone	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	Internal	10.0.49.1	255.255.0.0	Transparent Mode	100 Mbps half-duplex		
X1	External	10.0.49.1	255.255.0.0	Static	100 Mbps half-duplex		
X2	Management	192.168.168.168	255.255.255.0	Static	No link	Management Interface	
X3	HF-Link	N/A	N/A	N/A	No link	Hardware Failover Link	

Click [here](#) to verify your network settings.

#### Routing Table

IP Address Range	Gateway	Interface	Configure
No Entries			
<a href="#">Add</a>	<a href="#">Delete All</a>		

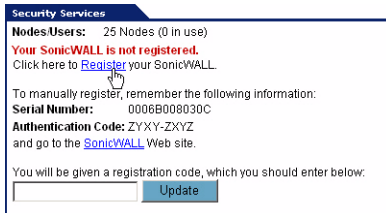


**Note:** mySonicWALL.com registration information is not sold or shared with any other company.

## Creating a mySonicWALL.com Account

Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form in the SonicWALL CSM management interface. You must have your SonicWALL CSM and your management station connected to the Internet to complete the online registration process. If you already have a mysonicWALL.com account, refer to “Registering Your SonicWALL CSM Using the Management Interface” on page 20.

1. If you are not logged into the SonicWALL CSM management interface, log in with the SonicWALL CSM administrative user name and password.
2. The **System > Status** page automatically displays. If the **System > Status** page does not automatically display, click **System** in the left-navigation menu, and then click **Status**.
3. On the **System > Status** page, in the **Security Services** section, click the **Register** link in **Your SonicWALL is not registered. Click here to Register your SonicWALL.**



4. In the **mySonicWALL.com Login** page, click the **here** link in “If you do not have a mySonicWALL account, please click **here** to create one.” The mySonicWALL.com account form is displayed.



5. In the **mySonicWALL Account** page, enter in your information in the **Account Information**, **Personal Information** and **Preferences** fields. All fields marked with an asterisk (\*) are required fields. Be sure to remember your username and password to access your mySonicWALL.com account.
6. Click **Submit** after completing the **mySonicWALL Account** form.
7. When the mySonicWALL.com server has finished processing your account, you will see a page saying that your account has been created. Click **Continue**. Your mySonicWALL.com account is activated. Now you need to log into mySonicWALL.com to register your SonicWALL CSM.

## Registering Your SonicWALL CSM Using the Management Interface

1. Log in to the SonicWALL CSM management interface if you are not logged in.
2. If the **System > Status** page is not displayed in the management interface, click **System** in the left-navigation menu, and then click **Status**.
3. On the **System > Status** page, in the **Security Services** section, click the **Register** link in the sentence **Click here to Register your SonicWALL**. The **mySonicWALL.com Login** page is displayed.
4. Enter your mySonicWALL.com account username and password in the **User Name** and **Password** fields, then click **Submit**.
5. At the top of the **Product Survey** page, Enter a “friendly name” for your SonicWALL CSM appliance in the **Friendly Name** field. The friendly name allows you to easily identify your SonicWALL content security appliance in your mySonicWALL.com account.
6. Please complete the Product Survey. SonicWALL uses this information to further tailor services to fit your needs.
7. Click **Submit**.
8. When the mySonicWALL.com server has finished processing your registration, you will see a page informing you that your SonicWALL CSM appliance is registered. Click **Continue**, and the **System > Licenses** page is displayed showing you all your activated services.

## Congratulations

Your SonicWALL CSM is now fully operational, filtering HTTP content for all users. At this point, all network user traffic on the network segment is filtered using the pre-configured **\*Default Policy**, which automatically applies the following Web filter categories to all users: **Adult Content**, **Drugs/Alcohol/Tobacco**, and **Racism/Hate/violence/Weapons**. For more information on the \*Default Policy, refer to “Understanding the \*Default Policy” on page 21.

For information on modifying the \*Default Policy to block more objectionable content categories, refer to the [SonicOS CF 2.5 Administrator's Guide](#).

The SonicWALL CSM also provides application filtering, which can block application traffic from the following:

- IM (Instant Messaging) applications
- P2P (Peer-to-Peer) applications
- Multimedia applications

For more information on configuring application filters, refer to the [SonicOS CF 2.5 Administrator's Guide](#).

## Understanding the \*Default Policy

The SonicWALL CSM includes a pre-configured \*Default Policy with pre-defined Web Filter Category Sets. The default settings are automatically applied when you add users from the network segment protected by the SonicWALL CSM, unless you assign a custom filtering policy to them.

You can use the \*Default Policy and its pre-configured Web Filter Category Sets as a base-line defense, providing the highest level of content filtering to all users. The \*Default Policy is initially configured to block the most common objectionable content categories, including:

- **Adult Content** - Sites that contain material of adult nature that may or may not contain excessive violence, sexual content, or nudity. These sites include profane or vulgar content and sites that are not appropriate for children.
- **Drugs/Alcohol/Tobacco** - Sites that promote or offer alcohol/tobacco products for sale, or provide the means to create them. Also includes sites that glorify, tout, or otherwise encourage the consumption of alcohol or tobacco. Sites that promote, offer, sell, supply, encourage or otherwise advocate the illegal use, cultivation, manufacture, or distribution of drugs, pharmaceuticals, intoxicating plants or chemicals and their related paraphernalia. Does not include sites that sell alcohol or tobacco as a subset of other products.
- **Racism/Hate/violence/Weapons** - Sites that depict extreme physical harm to people or property, or that advocate or provide instructions on ways to cause such harm. Also includes sites that advocate, depict hostility or aggression toward, or denigrate an individual or group based on the basis of race, religion, gender, nationality, ethnic origin, or other involuntary characteristics.
- **Safe Search Enforcement** - Enables the strictest filtering on all searches on search engines like Google and Yahoo that offer some form of safe-search filtering.



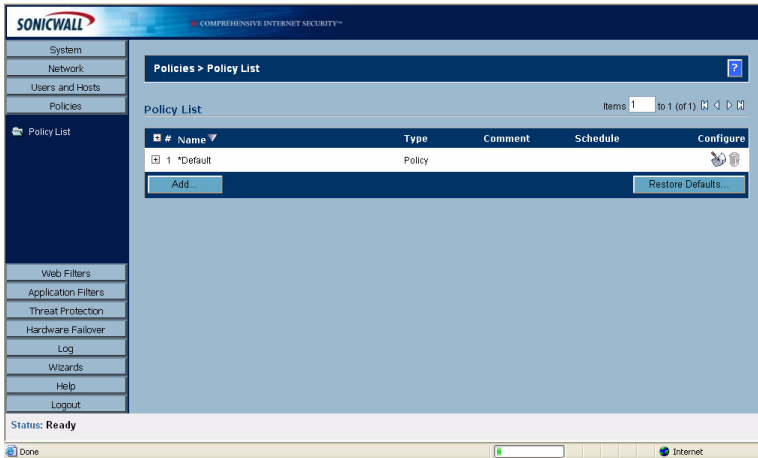
---

**Note:** Refer to the *[SonicOS CF 2.5 Administrator's Guide](#)* for a detailed description of all SonicWALL Content Filtering Service \*Default Policy categories, including instructions on modifying the \*Default Policy and creating new policies with customized Web and application filters.

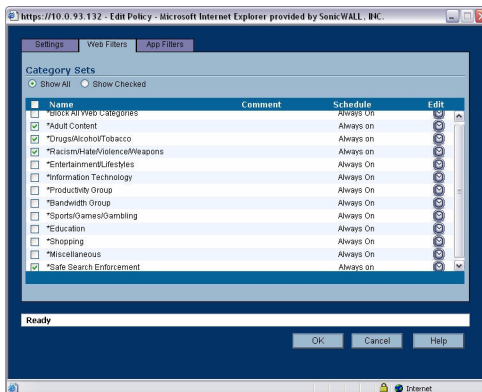
---

## Viewing the \*Default Policy Settings

1. In the management interface, click the **Policies** tab, then select **Policy List**.



2. Click the **Configure** icon next to **\*Default**.
3. To view the default Web filters, click the **Web Filters** tab. The **\*Default** Web filters are **Adult Content**, **Drugs/Alcohol/Tobacco**, and **Racism/Hate/Violence/Weapons** and **Safe Search Enforcement**. These Web filters will be checked by default.



4. To view application filters, click the **App Filters** tab. There are no default filters, so no filters will be checked. For more detailed configuration of application filters, refer to the [SonicOS CF 2.5 Administrator's Guide](#). If this screen appears without the names of the optional application filters, you need to re-register your appliance. Refer to ["Registering Your SonicWALL CSM Using the Management Interface"](#) on [page 20](#).

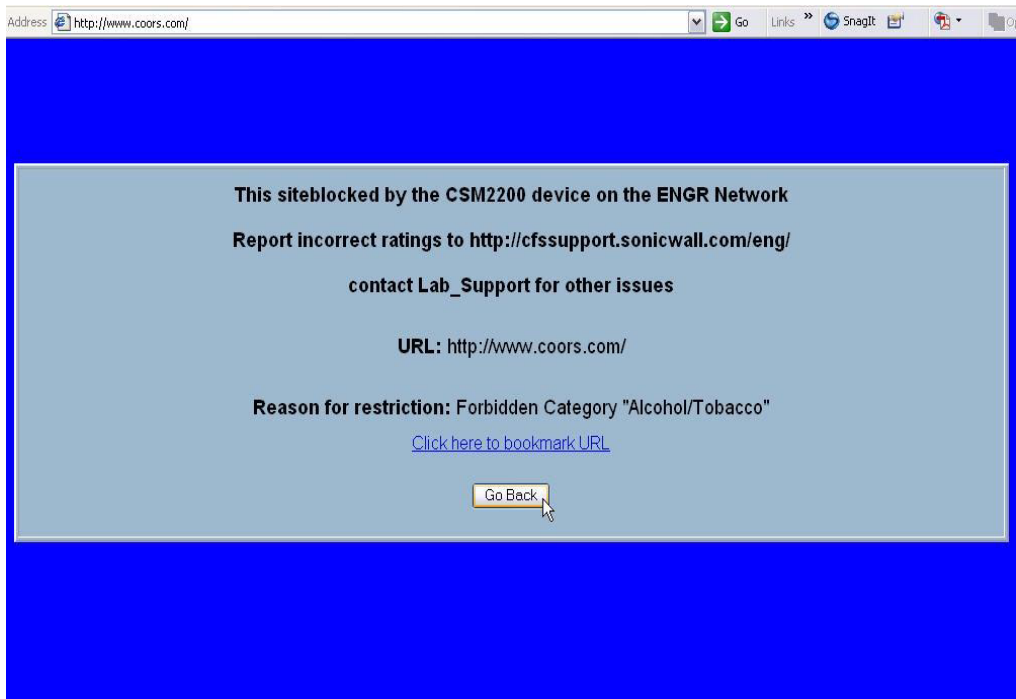
## 7

## Verifying the \*Default Policy

You can verify that the \*Default Policy is active by testing the each default Web filter category using a computer with an IP address that is within the assigned IP address range you specified in **Users and Hosts > Hosts** and that is on the same LAN as the SonicWALL CSM. For each \*Default Policy Web filter category, visit a well-known Web site in that category. If the SonicWALL CSM has been correctly configured, you will see a page indicating that the site has been blocked by policy.

- To test the **Adult Content** filter, visit a well-known Web site in that category, for example, <www.playboy.com>.
- To test the **Drugs/Alcohol/Tobacco** filter, visit a well-known Web site in that category, for example, <www.coors.com>.
- To test the **Racism/Hate/Violence/Weapons** filter, visit a well-known Web site in that category, for example, <www.winchester.com>.

If the SonicWALL CSM has been correctly configured, for each Web site you test, you will see the message, “This site has been blocked by policy.”



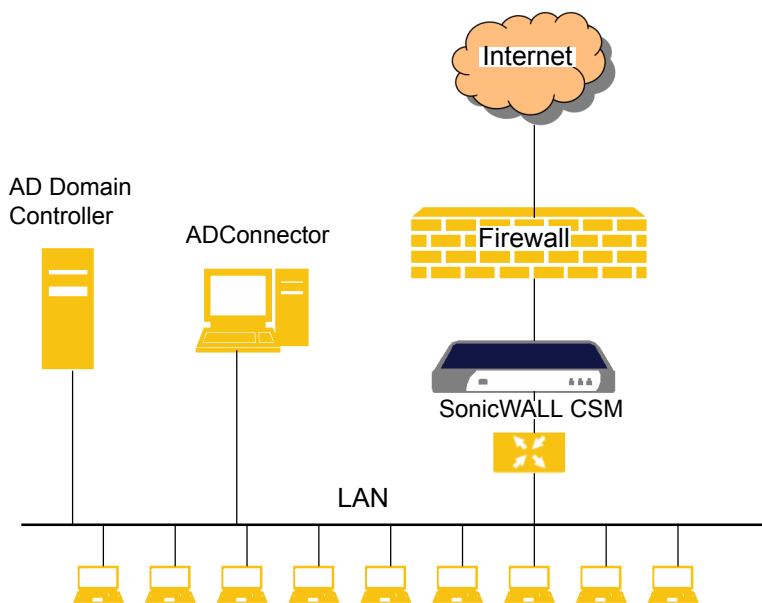


## Integrating the SonicWALL CSM with Microsoft Active Directory

To provide direct, single-sign-on integration with Microsoft's Active Directory for applying filtering properties, the SonicWALL CSM includes the SonicWALL ADConnector application to provide an interface between the SonicWALL CSM filtering policies and Active Directory.

**Note:** Refer to the *SonicWALL Content Security Manager Integrated Solutions Guide* for complete instructions on installing, configuring and using the SonicWALL ADConnector application.

The following instructions assume Active Directory is fully operational on your network.



**Note:** If you are not using Active Directory, the SonicWALL CSM includes a built-in Category Set authentication database. Refer to the *SonicOS CF 2.5 Administrator's Guide*.

## SonicWALL ADConnector Requirements

The Windows PC on which you install the SonicWALL ADConnector must meet the following requirements:

- A direct or routable access to both the Active Directory Domain Controller and the SonicWALL CSM
- An always on computer, so that the SonicWALL CSM can communicate with the Windows computer as needed
- A computer that belongs to the domain against which the authentication occurs

## Information You Need to Install and Configure Your SonicWALL ADConnector

Use the following information to install and configure the SonicWALL ADConnector:

- SonicWALL CSM **X0/X1** interface IP address: \_\_\_\_\_
- SonicWALL CSM ADConnector Configuration port number: \_\_\_\_\_
- SonicWALL CSM ADConnector Configuration shared secret: \_\_\_\_\_  
The shared secret must be a 16-digit hexadecimal number, for example:  
*0123456789abcdef*
- IP address of the SonicWALL ADConnector workstation: \_\_\_\_\_
- Workstation administrator account name: \_\_\_\_\_
- AD Domain administrator account name: \_\_\_\_\_
- AD Domain administrator account password.

## Download SonicWALL ADConnector Software



---

**Note:** *You must register your SonicWALL CSM before you can download the SonicWALL ADConnector Software. For instructions registering, refer to “Registering Your SonicWALL CSM” on page 17.*

---

1. Go to <https://www.mySonicWALL.com> and log in.
2. Click **Download Center** under **Download** in the left-hand column.
3. In the **Type** drop-down list, select **Content Security Manager**.
4. In the **Available Software** list, download the SonicWALL ADConnector.

## Install the SonicWALL ADConnector

The SonicWALL ADConnector installation wizard installs both the SonicWALL ADConnector Configuration Tool and the SonicWALL Agent Service.



---


**Note:** *You must have administrative privileges on the computer where you are installing the SonicWALL ADConnector.*

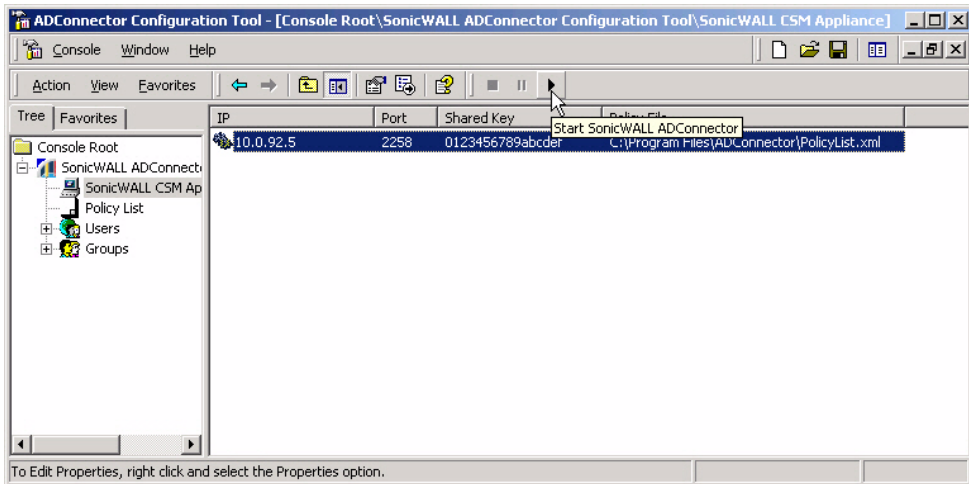
---

1. Launch the SonicWALL ADConnector setup program you downloaded from <https://mySonicWALL.com>.
2. You may be prompted to install the Microsoft.NET 1.1 Framework. Click **Yes**.
3. You may see a **Security Warning** dialog box asking if you want to accept a certificate from InstallShield Software Corporation. SonicWALL uses InstallShield® to install the SonicWALL ADConnector software. Click **Yes**.
4. If you are installing the Microsoft.NET framework, select **I Agree** in the **Microsoft.NET License Agreement** dialog box, then click **Install**. When Microsoft.NET installation is complete, the SonicWALL ADConnector installation wizard starts.
5. The **Welcome** page is displayed for the SonicWALL ADConnector. Click **Next**.
6. In the **License Agreement** page, click **I accept the terms in the license agreement** if you want to continue with the installation. Click **Next**.
7. On the **Customer Information** page, enter your name and organization. Click **Next**.
8. On the **Destination Folder** page, use the default directory or click on the **Change** button to specify another directory to install the program files. Click **Next**.
9. On the **Ready to Install the Program** page, click **Install**.
10. On the **ADConnector Configuration** page, enter:
  - **CSM Appliance IP** - the IP address of the SonicWALL CSM
  - **CSM Appliance Port** - the UDP port that will be used for communication between the two devices. The default is **2258**. This value will also be specified in **ADConnector Configuration** window in the SonicWALL CSM management interface.
  - **Shared Key** - the DES passphrase used to encrypt the communication between the devices. The Shared Key must be a 16-digit hexadecimal number, for example: *0123456789abcdef*.
11. Click **Next**.
12. On the **CFA User Configuration** page, enter information for the domain user account the SonicWALL ADConnector will use to log into the AD Domain Controller. The account must have AD administrator privileges. Enter the **ADConnector Username**, **ADConnector Password**, and **Domain Name**.
13. Click **Next**.
14. On the **Wizard Completed** page, click **Finish**.

## Starting the SonicWALL ADConnector

After installing the SonicWALL ADConnector, start the service. The agent service must be running at all times for the SonicWALL CSM to communicate with Active Directory.

1. On your Windows desktop, double click the **ADConnector Configuration Tool** icon, or from the Windows **Start** menu, select **Programs > SonicWALL > SonicWALL ADConnector > ADConnector Configuration Tool**. The ADConnector Configuration Tool launches. This is part of the Microsoft Management Console (MMC).
2. In the Console Root window, click the expand (+) icon next to **SonicWALL ADConnector Configuration Tool** in the left column to display its contents in the right column.
3. Underneath the **SonicWALL ADConnector Configuration Tool** in the left column, click the **SonicWALL CSM Appliance** icon.
4. Select the entry in the right window, and click the start button  in the toolbar above the entry.

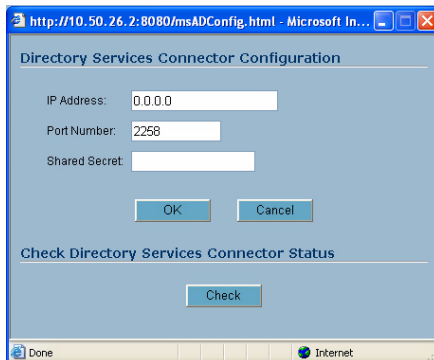


## Preparing the SonicWALL ADConnector Configuration Tool for First Use

1. Expand the **Users** list to view the users.
2. The first time you click on a user, the SonicWALL ADConnector prompts you for the Active Directory attributes for the SonicWALL ADConnector. Click **OK** in the Warning dialog box.
3. In the **Attribute Selection** dialog box, select attributes that are otherwise unused in on the system, for example, **IP Phone**. Select different attributes for the Category Set. Once the attributes have been selected, filtering policies for AD Category Sets can now be managed.

## Configuring the SonicWALL CSM for Microsoft Active Directory

1. In the SonicWALL CSM management interface, select **Users and Hosts > Settings**.
2. In the **Authentication Method** section, select **Use Directory Services Connector** and click the **Configure** button. The **SonicWALL Directory Services Connector Configuration** window is displayed.



3. Enter the IP address of the computer/server running the Directory Services Connector in the **IP Address** field.
4. Enter a port number in the **Port Number** field.
5. In the **Shared Secret** field, enter the same as the shared key you configured for the SonicWALL ADConnector when you installed it. The shared secret must be a sixteen-digit hexadecimal number, for example, *0123456789abcdef*.
6. Click **OK** to apply the configuration.
7. In the **Users and Hosts > Settings** page, click **Configure** for Directory Services Connector again.

8. Click **Check**. The Active Directory Agent Status window is displayed. If the Directory Services Connector is detected, the message **Directory Services Connector is ready** is displayed.
9. Click **OK** twice to exit.

At the end of step 8, if you see the message, **Directory Services Connector is not responding**, test connectivity from the SonicWALL CSM to the SonicWALL ADConnector:

1. In the management interface, click **System** and then click **Diagnostics**.
2. In the **System > Diagnostics** page, Select **Ping** from the **Diagnostic Tool** list.
3. In the **Ping host or IP address** field, enter the IP address of your SonicWALL ADConnector and click **Go**.
  - If the SonicWALL Directory Services Connector is not responding check that the computer with the SonicWALL ADConnector is turned on and has internet connectivity. Then ping it again.
  - If the SonicWALL Directory Services Connector is not responding or is alive but has a very long ping time (greater than 50 milliseconds), you should add a static route from the SonicWALL CSM to the SonicWALL ADConnector.
  - If the SonicWALL Directory Services Connector is alive with a fast ping time, your connectivity from the SonicWALL CSM to the SonicWALL ADConnector is good. Verify that the service is running and that the user you configured it with has sufficient privileges to communicate with the Active Directory domain controller.

## Adding a Static Route to the SonicWALL ADConnector

If the SonicWALL ADConnector is installed on a computer in a different subnet than the SonicWALL CSM, you need to add a static route in the SonicWALL CSM to the SonicWALL ADConnector station:

1. In the SonicWALL CSM management interface, in the left-navigation menu, click **Network** and then click **Interfaces**.
2. In the **Network > Interfaces** page, click **Add** below the **Route** table.
3. Click **Add** in the **Routing Table** section. The **Add Route** window is displayed.
4. Enter the beginning IP address of the IP address range to which the SonicWALL ADConnector belongs in the **IP Address From** field.
5. Enter the ending IP address of the IP address in the **IP Address To** field.
6. Enter the IP address of the gateway device to which the SonicWALL ADConnector is attached in the **Gateway IP** field.
7. Select **Internal (X0)** from the **Interface** menu.
8. Click **OK**. The static route entry is added to the **Routing Table**.



---

**Note:** *For instructions on assigning filter policies to users in Active Directory, refer to the SonicOS CF 2.5 Administrator's Guide.*

---



## Advanced Configuration

After you initially set up and configure your SonicWALL CSM, these are the key steps you take to provide content filtering to your LAN:

1. Organize your Web Filters and determine the content filtering needs for each Category Set. These can be local users, RADIUS users, or Active Directory users.
2. Create content filtering policies using the default categories, custom categories and web risks. You can create new policies or modify the twelve default policies.
3. Assemble the policies into Category Sets to meet the needs of each user.
4. Apply the appropriate Category Set.
5. Determine if any of your users have content filtering needs different from the needs of the Category Set they belong to, and assign an appropriate policy or Category Set to each exceptional user.
6. Determine the application filtering needs of your LAN and configure application filters. For example, do you want to block instant messaging or streaming video?
7. Create usage reports using the SonicWALL ViewPoint application (available for download from <https://www.mysonicwall.com>).
8. If you are protecting multiple subnets, create static routes between the SonicWALL CSM and servers in the different subnets.



---

**Note:** *For more information on these advanced configuration procedures, refer to the SonicOS CF 2.5 Administrator's Guide.*

---

# Configuring Static IP

To configure the static IP address and subnet mask on your management station, follow the steps below:

## Windows XP

1. Right click the **Local Area Connection** icon and select **Properties**.
2. Double-click **Internet Protocol (TCP/IP)**.
3. In the Internet Protocol (TCP/IP) Properties window, select **Use the following IP address** and type an available IP address, for example, **192.168.168.20**.
4. Type **255.255.255.0** in the **Subnet Mask** field.
5. Click **OK** for the settings to take effect.

## Windows 2000

1. From your Start menu, select **Settings**.
2. Open **Network and Dial-up Connections**.
3. Click **Properties**.
4. Highlight **Internet Protocol (TCP/IP)** and click **Properties**.
5. Select **Use the following IP address**.
6. Type an available IP address, for example, **192.168.168.20** in the **IP address** field.
7. Type **255.255.255.0** in the **Subnet** field.
8. Click **OK** for the settings to take effect.

## Windows NT

1. From the Start menu, highlight **Settings** and then select **Control Panel**.
2. Open **Network**.
3. Double-click **TCP/IP** in the TCP/IP Properties window.
4. Select **Specify an IP Address**.
5. Type an available IP address, for example, **192.168.168.20** in the **IP Address** field.
6. Type **255.255.255.0** in the **Subnet Mask** field.
7. Click **OK**, and then click **OK** again.
8. Restart the computer for changes to take effect.

## Windows 98

1. In the Start menu, select **Settings** and then select **Control Panel**.
2. Open **Network**.
3. **Double-click** **TCP/IP** in the TCP/IP Properties window.
4. Select **Specify an IP Address**.
5. Type an available IP address, for example, **192.168.168.20** in the **IP Address** field.
6. Type **255.255.255.0** in the **Subnet Mask** field.
7. Click **OK**, and then click **OK** again.
8. Restart the computer for changes to take effect.

# Glossary of Networking Terms

**SonicWALL ADConnector** - A SonicWALL application for integrating SonicWALL Content Security Manager filtering policies with Microsoft Active Directory groups and users.

**application filtering** - A signature-based deep packet inspection mechanism for controlling peer-to-peer (P2P), Instant Messaging (IM), and Multimedia applications usage.

**content filtering (CF)** - A method of screening Web pages and email messages to exclude specified users from access to them, using special filtering policies. The policies use a variety of exclusion criteria including character string matching or source IP address matching. Additionally, the policies contain priority levels, indicating sensitivity of content.

**Content Security Manager (CSM)** - A SonicWALL Internet content and application filtering solution that enhances security and employee productivity, optimizes network bandwidth and mitigates legal liabilities.

**default gateway** - A device on an internetwork that forwards packets to another network.

**DNS** - Domain Name System, a hierarchical naming system that resolves a domain name with its associated IP address. A DNS server looks up the name of a computer and finds the corresponding IP address. This allows users to access hosts using friendly text-based names instead of IP addresses. These names are called fully qualified domain names (FQDN).

**hardware failover** - The capability of a mission-critical device, such as a SonicWALL CSM, to automatically failover to a backup device in the event of a hardware failure on the primary unit.

**IP address** - Internet Protocol Address, a thirty-two bit number that identifies a computer or other resource on the Internet or on any TCP/IP network. The number is usually expressed as four numbers from 0 to 255 separated by periods, for example, 172.16.31.254.

**LAN** - A Local Area Network is typically a group of computers located at a single location, and is commonly based on the Ethernet architecture.

**packet** - A unit of information transmitted over the internet or within any TCP/IP network. Packets have a header, which contains information about the source, destination, and protocol to be used for the data, and a body, which contains the data being transmitted.

**private IP address** - An IP address for a resource in your network that is not known or published outside the zone (for example LAN) where it is located.

**public IP address** - An IP address for a resource in your network that is published outside your network to the WAN.

**router** - A device that routes data between networks through IP address information in the header of the IP packet. A router forwards packets to other routers until the packets reach their destination. The Internet is the largest example of a routed network.

**subnet** - A portion of a network. Each subnet within a network shares a common network address and is uniquely identified by a subnetwork number.

**subnet mask** - A 32-bit number used to separate the network and host sections of an IP address. A subnet mask subdivides an IP network into smaller pieces. An example of a subnet mask might be 255.255.255.248 for subnet with only eight IP addresses.

**TCP/IP** - Transmission Control Protocol/Internet Protocol is the basic communication protocol of the Internet. It supports sending information in packets, and identifies each device with a unique numeric IP address.

**WAN** - A Wide Area Network is a geographically distributed network composed of multiple networks joined into a single large network. The Internet is a global WAN.

# SonicWALL CSM Appliance Regulatory Statement and Safety Instructions

Regulatory Model/Type	Product Name
1RK0A-02A	CSM 2200

## FCC Part 15 Class A Notice

Note: This equipment was tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, the device may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user is required to correct the interference at his own expense.

Caution: Modifying this equipment or using this equipment for purposes not shown in this manual without the written consent of SonicWALL, Inc. could void the user’s authority to operate this equipment.

## Canadian Radio Frequency Emissions Statement

This Class A digital apparatus complies with Canadian ICES-003.Cet appareil numérique de la classe A est conforme à toutes la norme NMB-003 du Canada.

## CISPR 22 (EN 55022) Class A

Warning: This is a class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Complies with EN 55022 Class A and CISPR22 Class A.

## EU Declaration of Conformity

Application of council Directives 89/336/EEC (EMC) and 72/23/EEC (LVD)

Standards to which conformity is declared:

EN 55022 (1998) +A2 Class A

EN 55024 (1998) +A2

EN 61000-3-2 (2000)

EN 61000-3-3 (1995) +A1

EN 60950-1 (2001) + A11

National Deviations: AT, AU, BE, CH, CN, CZ, DE, DK, FI, FR, GB, GR, HU, IE, IL, IN, IT, JP, KR, NL, NO, PL, SE, SG, SI

## BMSI Statement

警告使用者：

這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

## VCCI Statement

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用する  
と電波妨害を引き起こすことがあります。この場合には使用者が適切な対策  
を講ずるよう要求されることがあります。

**VCCI— A**

## Regulatory Information for Korea



Ministry of Information and Telecommunication

All products with country code "" (blank) and "A" are made in the USA.

All products with country code "B" are made in China.

All products with country code "C" "D" or "F" are made in Taiwan R.O.C.

All certificates held by NetSonic, Inc.

### A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니 판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약 잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기 바랍니다.

## Lithium Battery Warning

The Lithium Battery used in the SonicWALL Internet security appliance may not be replaced by the user. Call SonicWALL technical support in U.S./Canada at 888-777-1476 or visit the SonicWALL Web site at <<http://www.sonicwall.com>> for international customer support telephone numbers. If, for any reason, the battery or SonicWALL Internet security appliance must be disposed of, do so following the battery manufacturer's instructions.

## Cable Connections

All Ethernet and RS232 (Console) cables are designed for intra-building connection to other equipment. Do not connect these ports directly to communication wiring or other wiring that exits the building where the SonicWALL is located.

## Mounting the SonicWALL CSM

The above SonicWALL appliances are designed to be mounted in a standard 19-inch rack mount cabinet. The following conditions are required for proper installation:

- Use the mounting hardware recommended by the rack manufacturer and ensure that the rack is adequate for the application. SonicWALL includes a rack mounting kit with the SonicWALL CSM that is compatible with most computer equipment racks.
- Four mounting screws, compatible with the rack design, must be used and hand tightened to ensure secure installation. Choose a mounting location where all four mounting holes line up with those of the mounting bars of the 19-inch rack mount cabinet.
- Mount in a location away from direct sunlight and sources of heat. A maximum ambient temperature of 104° F (40° C) is recommended.
- Route cables away from power lines, fluorescent lighting fixtures, and sources of noise such as radios, transmitters, and broadband amplifiers
- Ensure that no water or excessive moisture can enter the unit.
- The included power cord is intended for use in North America only. For European Union (EU) customers, a power cord is not included.
- Allow unrestricted airflow around the unit and through the vents on the side of the unit. A minimum of 1 inch (25.44mm) clearance is recommended.
- Mount the SonicWALL appliances evenly in the rack in order to prevent a hazardous condition caused by uneven mechanical loading.
- Consideration must be given to the connection of the equipment to the supply circuit and the effect of overloading the circuits has minimal impact on overcurrent protection and supply wiring. Appropriate consideration of equipment nameplate ratings must be used when addressing this concern.
- Reliable grounding of rack-mounted equipment must be maintained. Particular attention must be given to power supply connections other than direct connections to the branch circuits such as using power strips.

## German Language Regulatory and Safety Instructions

### Hinweis zur Lithiumbatterie

Die in der Internet Security appliance von SonicWALL verwendete Lithiumbatterie darf nicht vom Benutzer ausgetauscht werden. Zum Austauschen der Batterie muss die SonicWALL in ein von SonicWALL autorisiertes Service-Center gebracht werden. Dort wird die Batterie durch denselben oder entsprechenden, vom Hersteller empfohlenen Batterietyp ersetzt. Beachten Sie bei einer Entsorgung der Batterie oder der SonicWALL Internet Security appliance die diesbezüglichen Anweisungen des Herstellers.



## Kabelverbindungen

Alle Ethernet- und RJ45 Konsole-Kabel eignen sich für die Verbindung von Geräten in Innenräumen. Schließen Sie an die Anschlüsse der SonicWALL keine Kabel an, die aus dem Gebäude herausgeführt werden, in dem sich das Gerät befindet.

## Weitere Hinweise zur Montage der Modell

Die oben genannten SonicWALL-Modelle sind für eine Montage in einem standardmäßigen 19-Zoll-Rack konzipiert. Für eine ordnungsgemäße Montage müssen die folgenden Bedingungen erfüllt werden:

- Vergewissern Sie sich, dass das Rack für die Anwendung geeignet ist, und verwenden Sie das vom Rack-Hersteller empfohlene Montagezubehör.
- Verwenden Sie für eine sichere Montage vier passende Befestigungsschrauben, und ziehen Sie diese mit der Hand an. Montieren Sie das Gerät so, dass sich die Anordnung der Montagelöcher mit den Löchern der Träger im 19-Zoll-Rack deckt.
- Wählen Sie für die Montage einen Ort, der keinem direkten Sonnenlicht ausgesetzt ist und sich nicht in der Nähe von Wärmequellen befindet. Die Umgebungstemperatur darf nicht mehr als 40 °C betragen.
- Führen Sie die Kabel nicht entlang von Stromleitungen, Leuchtstoffröhren und Störquellen wie Funksendern oder Breitbandverstärkern.
- Das eingeschlossene Netzkabel ist für Gebrauch in Nordamerikas nur vorgehabt. Für Europäische Union (EU) Kunden, ist ein Netzkabel nicht eingeschlossen.
- Stellen Sie sicher, dass das Gerät vor Wasser und hoher Luftfeuchtigkeit geschützt ist.
- Stellen Sie sicher, dass die Luft um das Gerät herum zirkulieren kann und die Lüftungsschlitze an der Seite des Gehäuses frei sind. Hier ist ein Belüftungsabstand von mindestens 26 mm einzuhalten.
- Bringen Sie die SonicWALL gerade im Rack an, um mögliche Gefahren durch ungleiche mechanische Belastung zu vermeiden.
- Prüfen Sie den Anschluss des Geräts an die Stromversorgung, damit der Überstromschutz sowie die elektrische Leitung nicht von einer eventuellen Überlastung der Stromversorgung beeinflusst werden. Prüfen Sie dabei sorgfältig die Angaben auf dem Aufkleber des Geräts.
- Vergewissern Sie sich, dass das Gerät sicher im Rack befestigt ist. Insbesondere muss auf nicht direkte Anschlüsse an Stromquellen geachtet werden wie z. B. bei Verwendung von Mehrfachsteckdosen.

# Copyright Notice

© 2006 SonicWALL, Inc.

All rights reserved.

Under the copyright laws, this manual or the software described within, cannot be copied, in whole or part, without the written consent of the manufacturer, except in the normal use of the software to make a backup copy. The same proprietary and copyright notices must be affixed to any permitted copies as were affixed to the original. This exception does not allow copies to be made for others, whether or not sold, but all of the material purchased (with all backup copies) can be sold, given, or loaned to another person. Under the law, copying includes translating into another language or format.

Specifications and descriptions subject to change without notice.

## Trademarks

SonicWALL is a registered trademark of SonicWALL, Inc.

Microsoft Windows 98, Windows NT, Windows 2000, Windows XP, Windows Server 2003, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

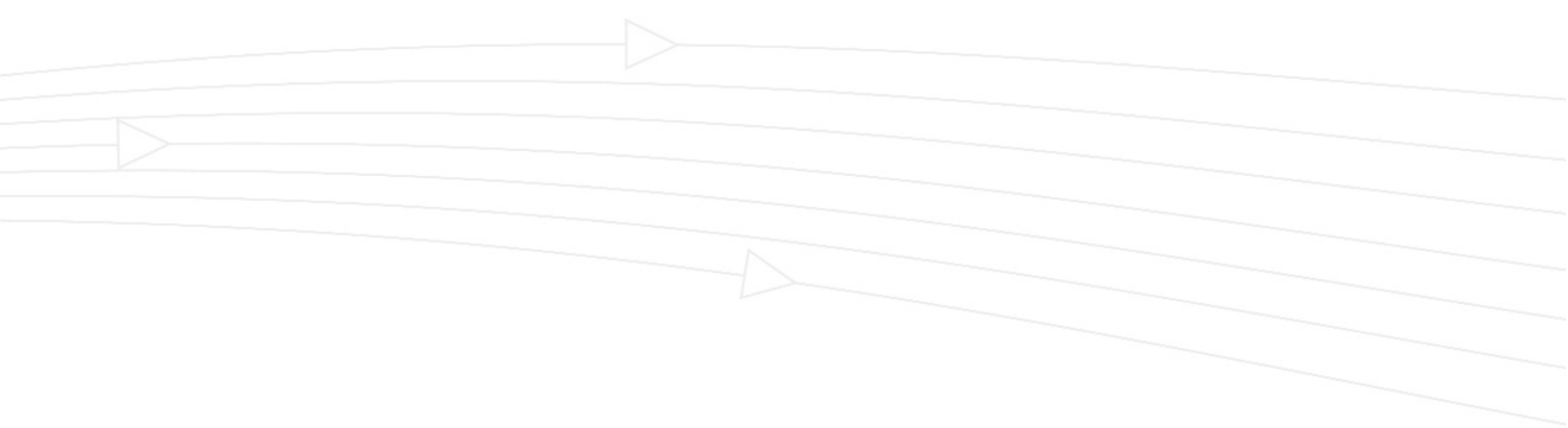
Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the U.S. and/or other countries.

Firefox is a trademark of the Mozilla Foundation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

# Notes



**SonicWALL, Inc.**

1143 Borregas Avenue  
Sunnyvale, CA 94089-1306

T: 408.745.9600  
F: 408.745.9300

[www.sonicwall.com](http://www.sonicwall.com)

© 2006 SonicWALL, Inc. SonicWALL is a registered trademark of SonicWALL, Inc. Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies. Specifications and descriptions subject to change without notice.

P/N 232-000017-00  
Rev A 06/06

